Governance and Risk Management

Provide in Advance	1. A copy of Registrant's organization chart showing ownership percentages of Registrant and control persons, and a schedule or chart of all affiliated entities. Include all entities that are commonly controlled by, or under common control with, the Registrant.
Provide in Advance	2. List of all office locations, including Registrant's principal office and place of business ("Main Office") and any other locations from which Registrant routinely conducts investment advisory services ("Branch Offices"). For each location, provide the address, date office opened, and number of employees and investment adviser representatives ("IARs") at the location.
Provide in Advance	3. List of current employees (including on-site contractors under the supervision of the adviser), IAR, partners, officers, and/or directors and their respective titles, department, office location, and employment/contract start date.
Provide in Advance	4. List of terminated employees and IARs, including name, title, and date of termination.
Provide in Advance	5. Organizational charts that illustrate the positions and departments responsible for cybersecurity-related matters and where these individuals and departments fit within the Registrant's organization or hierarchy.
Provide in Advance	6. Identify the Chief Information Security Officer or equivalent position. If the role does not exist, explain where the principal responsibility for overseeing cybersecurity resides within the Registrant.
Provide in Advance	7. Provide a copy of firm policies and procedures addressing the protection of client records and information, including those that are designed to secure client documents and information; protect against anticipated threats to client information; protect against unauthorized access to client accounts or information; and address the storage and transmission (outside Registrant's network or Registrant's office) of client NPI by its branch offices and IARs for the Examination Period. *Please note that subsequent questions in this Request Letter may ask for policies and procedures that are covered by the documents produced in response to this question. For those questions, reference this question and specifically indicate where the information can be found within the documents produced.*
Provide in Advance	8. A copy of Registrant's privacy policy provided to clients during the Examination Period.
	9. A record of any non-compliance with Registrant's cybersecurity policies and

Provide in Advance	procedures during the Examination Period and any action taken as a result of such non-compliance.
Provide in Advance	10. A record of any client / investor complaints during the Examination Period involving cybersecurity or privacy. Please include a brief description of the resolution of the complaints and any remediation efforts undertaken in response.
Provide in Advance	11. Provide a copy of Registrant's policies and procedures related to penetration testing.
Provide in Advance	12. Provide a copy of Registrant's policies and procedures related to vulnerability scans.
Provide in Advance	13. Provide a copy of Registrant's policies and procedures for patch management, including procedures designed to ensure the prompt installation of critical patches. Also provide documentation (e.g., a sample log or report) evidencing patch maintenance tracking.
Make Available On-Site	14. A copy of Registrant's most recent assessment of its cybersecurity risks.
Make Available On-Site	15. Any annual or interim reports or other documents regarding the review or testing of Registrant's compliance with its cybersecurity policies and procedures, including those policies related to penetration testing, vulnerability scanning, and patch management.
Provide in Advance	16. Provide a copy of Registrant's policies and procedures relating to data classification. Please include a list of the types of data classification, the risk level (e.g., low, medium, or high) associated with each data classification, and a description of how the factors and risks are considered when determining whether data fits within each classification.
Make Available On-Site	17. Provide a copy of Registrant's policies and procedures related to verification of the authenticity of a client request to transfer funds. If no such written policies or procedures exist, please describe the process Registrant follows to verify the authenticity of fund transfer requests and describe the individuals and/or departments involved in the authentication process.
Provide in Advance	18. Provide a copy of Registrant's Regulation S-ID policy.
Make Available On-Site	19. Provide a copy of all minutes and briefing material provided to the Registrant's board of directors (or senior management if the Registrant does not have a board of directors) regarding cybersecurity, including any testing of the Registrant's cybersecurity program, actual cybersecurity incidents, assessment of cybersecurity risks, and changes to its client privacy policy or cybersecurity program and policies and procedures.

Access Rights and Controls

Make Available On-Site

20. Provide a copy of Registrant's inventory identifying where and how client NPI is maintained or stored, including a list of all third-party systems that are used to store client NPI.

Provide in Advance

21. Provide a copy of Registrant's policies and procedures that address the following:

Provide in Advance

a. Ensuring that unauthorized persons do not access its network resources and devices;

Provide in Advance

b. Restricting user (i.e., employee, IAR, contractor/vendor, other third parties) access based on role or job functions (e.g., access control policy, acceptable use policy, administrative management of systems, and corporate information security policy);

Provide in Advance

c. Updating access rights based on personnel or system changes (i.e., obtaining authorization to add, delete, or modify authorized user access to systems or applications);

Provide in Advance

d. Obtaining manager approval of changes to access rights or controls; and

Provide in Advance

e. Any ongoing review to ensure access rights continue to be accurately assigned.

Provide in Advance

If different policies and procedures apply to remote offices, IARs, contractors/vendors, or other third parties please provide those policies and procedures.

Provide in Advance

22. In reference to 21.b through 21.d, please also provide the following:

Provide in Advance

a. For establishing access rights: a list of the last ten employees or IARs who were hired by Registrant during the Examination Period, including:
    - employee/IAR name;
    - title;
    - employment hire date;
    - employment start date;
    - access rights and date access rights granted; and
    - documentation evidencing manager approval.

Provide in Advance

b. For updating access rights: (1) a list of the last ten employees or IARs to leave Registrant during the Examination Period and documentation evidencing their last date of employment and the date their access to Registrant's network and systems was terminated and (2) a list of the last ten employees or IARs to be reassigned by Registrant to a new group or function during the Examination Period and documentation evidencing:
    - the date of employee's/IAR's reassignment,
    - manager approval of change in access rights including date manager approved change, and
    - the date employee's/IAR's access to Registrant's systems and applications was modified.

Provide in Advance

23. If Registrant conducts reviews of user (i.e., employee, IAR, contractor/vendor, other third parties) access rights and restrictions with respect to role or job-specific resources within the network, provide a list of

reviews conducted during the Examination Period and a brief description of each. If Registrant maintains documentation related to these reviews, provide a copy of the most recent report for each type of review.

Provide in Advance

24. Provide a list of any instances during the Examination Period where system users (including employees, IARs, clients, contractors/vendors, and any other third parties) received entitlements or access to Registrant's network, data, systems, or reports in contravention of Registrant's policies or practices and without authorization. Please include the date and a brief description of the instance and any remediation efforts undertaken in response.

Make Available on-Site

25. Provide a list of the systems or applications for which Registrant uses multi-factor authentication for employee, IAR, contractor/vendor, other third parties, and client access. Also provide a list of the systems or applications for which Registrant does not use multi-factor authentication.

Provide in Advance

26. Provide a copy of Registrant's policies, procedures, and standards related to login attempts, failures, lockouts, and unlocks or resets. Please indicate how these policies are enforced.

Provide in Advance

27. Provide a list of all logs and reports that Registrant uses to review for failed log-in attempts, access lockouts, dormant user accounts, and unauthorized log-in attempts during the Examination Period. Please provide a description of each log or report, frequency in which it is generated and reviewed, and individual/department responsible for reviewing report or log.

Make Available On-Site

a. Provide a sample of each log and report utilized during the Examination Period.

Provide in Advance

28. Provide a copy of Registrant's policies, procedures, and standards regarding any devices (i.e., Registrant-issued and personal devices) used by employees, IARs, contractors/vendors, and/or other third parties to access Registrant's system externally including any written policies or procedures addressing the encryption of such devices and the Registrant's ability to remotely monitor, track, and deactivate remote devices.

Data Loss Prevention

Provide in Advance

29. Provide a copy of Registrant's enterprise data loss prevention policies and procedures, including, monitoring of external removable storage devices, and employees'(including on-site contractors under the supervision of the adviser) and IARs' use of personal devices.

Provide in Advance

30. Provide a list of the systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to client NPI. Please include a brief description of their functions and whether the systems are proprietary, managed by a third party, or commercial off-the-shelf products.

Provide in Advance

31. Provide a copy of Registrant's policies and procedures relating to monitoring exfiltration and unauthorized distribution of client NPI outside of Registrant through email, physical media, hard copy, web-based file transfer programs,

or via other electronic means. If Registrant maintains documentation of this monitoring, please include a copy of the most recent report.

Vendor Management

Provide in Advance

32. Provide a copy of Registrant's policies, procedures, and standards relating to contracting with third-party vendors, including cloud service providers (collectively, "Vendors"). If no written policies or procedures exist, please describe Registrant's processes related to Vendor selection, management, and oversight.

Make Available On-Site

33. Provide a list of all Vendors with access to Registrant's network, systems, or data including a brief description of the service (or type of service) the Vendor provides to Registrant, whether Registrant has access to client NPI, and whether Registrant has an executed contract in place with the Vendor.

Provide in Advance

a. Please provide a sample contract that illustrates the typical contractual terms related to Vendors' access to Registrant's networks, systems or data, including client NPI.

Provide in Advance

34. Provide a copy of any written contingency plans Registrant has with its Vendors in case of bankruptcy, the development of conflicts of interest, or other issues that might put the Vendor out of business. If not documented, please describe any such contingency plans (e.g., software escrow).

Provide in Advance

35. Provide a sample of documentation or notification that Registrant requires (or has received) from third-party Vendors to provide prior to any significant changes to the third-party Vendors' systems, components, or services that could potentially have security impacts to Registrant and its data containing NPI.

Provide in Advance

36. Provide a list of terminated Vendors during the Examination Period.

Training

Provide in Advance

37. Provide a list of any training offered by Registrant and/or third party vendors to its employees, IARs, and contractors/vendors during the Examination Period related to cybersecurity and risks. For each training, please identify the date(s) offered, topics, nature of the training method (e.g. in person, computer based learning, or email alerts), and groups of participants (i.e., employees, IARs, contractors/vendors). Please also provide a copy of any written guidance or training materials provided for each training.

Provide in Advance

38. Provide a copy of Registrant's cybersecurity training policies and procedures.

Incident Response

Provide in Advance

39. Provide a copy of Registrant's written plan that addresses mitigation of the

effects of a cybersecurity incident and/or recovery from such an incident, if such a plan exists. If Registrant maintains separate written cybersecurity incident response policies and procedures, please provide a copy.

Provide in Advance

40. Provide a copy of Registrant's policies and procedures for conducting tests or exercises of its incident response plan, including the frequency of such testing, if applicable.

Provide in Advance

41. If Registrant prepares a report related to testing of its incident response plan, please provide a copy of the most recent report.

Provide in Advance

42. Provide a list of all cybersecurity incidents or breaches that occurred during the Examination Period.

Provide in Advance

a. For those cybersecurity incidents that have been resolved and involved unauthorized distributions of client NPI, provide a brief description of each incident, including the date of occurrence, date discovered, and a description of any remediation efforts undertaken in response.

Make Available On-Site

b. For those cybersecurity incidents that have been <u>not</u> been resolved and involved unauthorized distributions of client NPI, provide a brief description of each incident, including the date of occurrence, date discovered, and a description of any remediation efforts in process.